

THE TOPOLOGY OF GROVER ALGORITHM

ALI NABI DUMAN

ABSTRACT. It has been shown in recent years that quantum information has a topological nature ([1], [2], [3]). In [7], Vicary undergoes the study of quantum algorithms using this new topological approach. The advantage of this new formalism is that it allows new proofs of correctness of the algorithms such as Deutsch-Jozsa, hidden subgroup and single-shot Grover algorithms. It also provide more clear insight to the generalizations of these algorithms. In this paper, we consider (multi-step) Grover algorithm from this new perspective.

1. INTRODUCTION

Recent works demonstrated that the quantum procedures can be examined more clearly using a topological approach rather than the classical presentations which utilize the matrices of complex numbers in an orderly manner ([1], [2], [3]). In this new approach pioneered by the works of Abramsky and Coecke one replaces the matrices with geometrical primitives.

Vicary has recently provided the topological analysis of Deutsch-Jozsa, hidden subgroup and single-shot Grover algorithms by overcoming the difficulties that come from the use of an oracle and group representation theory [7]. His work not only enable new and simple proofs of correctness but also produce new generalizations of these algorithms.

Date: May 20, 2014.

In [7], the author focuses on the case where a single iteration of the Grover algorithm is sufficient to find a marked element in a set. This algorithm can work correctly if exactly $\frac{1}{4}$ of the elements are marked. In this paper, we consider in a similar fashion the more general case where one element is marked in a set S of size 2^n . We perform $\sqrt{|S|}$ iteration using topological formalism.

This paper is organized as follows: In section 2, we explain conventional Grover algorithm. Section 3 is devoted to the topological semantics that we use in the paper. Finally, we give the presentation of the Grover algorithm using topological semantics and prove its correctness in section 4.

2. CONVENTIONAL GROVER SEARCH ALGORITHM

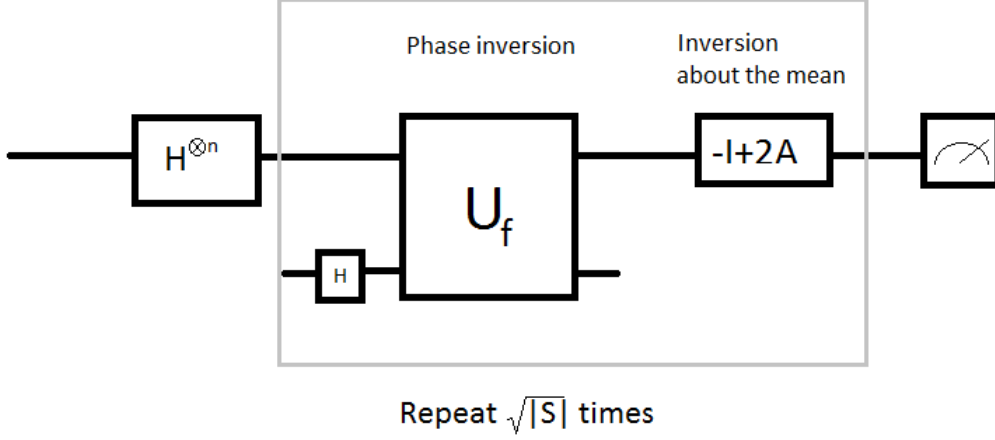
Grover search algorithm is introduced to find a marked element in an array $S = \{0, 1\}^n$ of size $|S| = 2^n$ (see [4]). The classical algorithms do this job in $|S|/2$ queries in average while it takes $\sqrt{|S|}$ queries for Grover search algorithm. The marked element x_0 is defined using an indicator function $f : S \rightarrow \mathbb{Z}_2$ where \mathbb{Z}_2 is the group of integers under addition modulo 2. Here $f(x)$ is equal to 1 for $x = x_0$ and to 0 for all other elements of S .

We then define the unitary operator $U_f : (\mathbb{C}^2)^n \otimes \mathbb{C}^2 \rightarrow (\mathbb{C}^2)^n \otimes \mathbb{C}^2$ as follows:

$$|x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes (|x\rangle \oplus |f(x)\rangle).$$

Here x is an element of S and y is an element of \mathbb{Z}_2 . The symbol \oplus is the addition in the group \mathbb{Z}_2 .

We can now introduce the quantum circuit for the Grover algorithm as follows:



where $H^{\otimes n}$ is n -fold Hadamard gate and the unitary matrix $-I+2A$ is the inversion about the mean. U_f and $-I+2A$ combined together separates the desired state after $\sqrt{|S|}$ consecutive applications. In other words, after $\sqrt{|S|}$ th step the probability of measuring any state except x_0 will be close to zero while probability of measuring x_0 will be greater than $1/2$. Hence, the final measurement in the algorithm will give us the desired element x_0 .

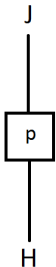
3. TOPOLOGICAL SEMANTICS

In this section we present topological semantics that we need to build the Grover algorithm. These geometric primitives correspond to properties of finite groups and finite sets. The content of this section can be found in the appendix of [7]. One can also refer to [5] and [6] for the mathematical foundation of the notation.

Here we start with the identity map on a finite Hilbert spaces. This is represented by a vertical wire.

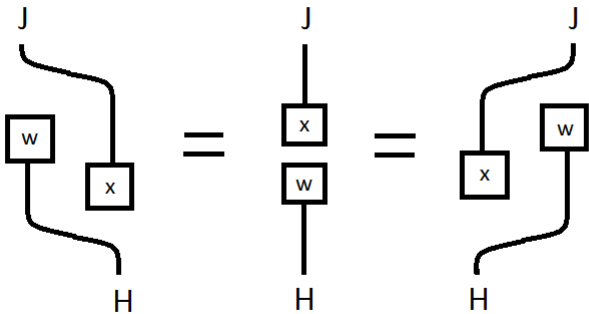


The following diagram represent a linear map $p : H \rightarrow J$.



The identity on the 1-dimensional Hilbert space is represented as the empty diagram:

One can change the relative heights of the boxes and move the components around.

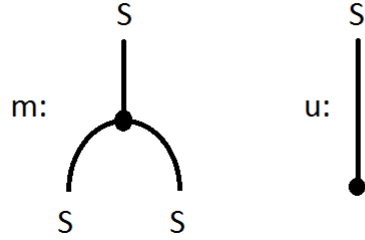


Let $\mathbb{C}[S]$ be the complex vector space whose basis elements are the elements of a finite set S . For the sake of brevity, we denote this vector space by S . Let $|s\rangle$ be a basis element of S . We define the maps $m : S \otimes S \rightarrow S$ and $u : \mathbb{C} \rightarrow S$ as follows:

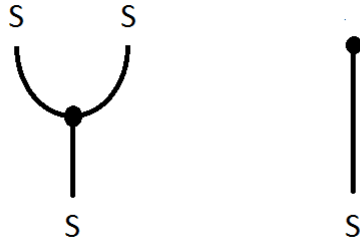
$$m(|i\rangle \otimes |j\rangle) := \delta_{i,j} |i\rangle$$

$$u := \sum_i |i\rangle.$$

The maps m and u gives S a commutative algebra structure and they are represented as follows:



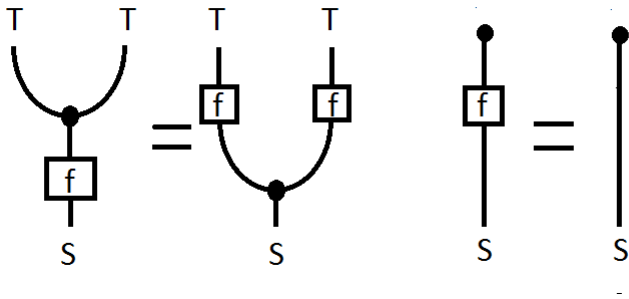
Their adjoints m^\dagger and u^\dagger are constructed in the following way:



A function $f : S \rightarrow T$ between finite sets extends to a linear map by $f|s\rangle := |f(s)\rangle$. The following diagram corresponds to this function:

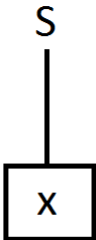


We have also morphisms with following two conditions

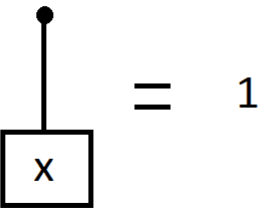


These are called *comonoid homomorphism* conditions.

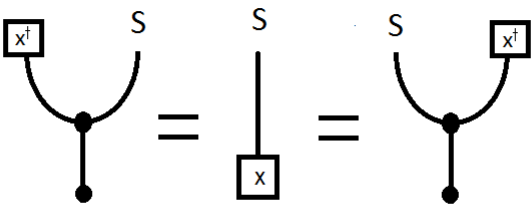
A chosen element $x \in S$ corresponds to a function $x : 1 \rightarrow S$, which we denote graphically as:



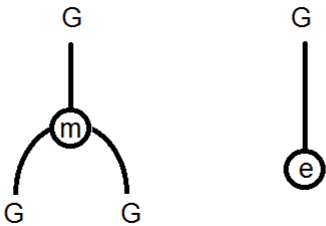
The deletion operator u^\dagger reduce the elements to unit scalars:


$$\begin{array}{c} \bullet \\ | \\ \boxed{x} \end{array} = 1$$

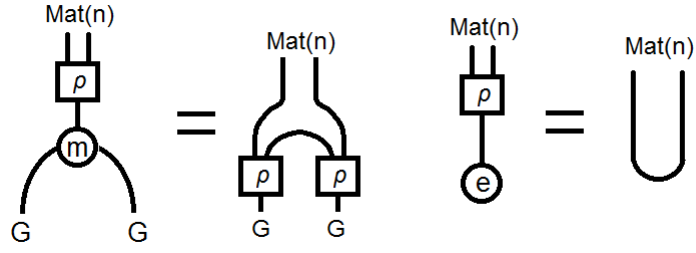
x and its adjoint x^\dagger are related as follows:


$$\begin{array}{c} \boxed{x^\dagger} \\ \curvearrowright \\ \bullet \\ | \\ \bullet \end{array} \stackrel{S}{=} \begin{array}{c} \bullet \\ | \\ \boxed{x} \end{array} \stackrel{S}{=} \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \begin{array}{c} \boxed{x^\dagger} \\ \curvearrowleft \end{array}$$

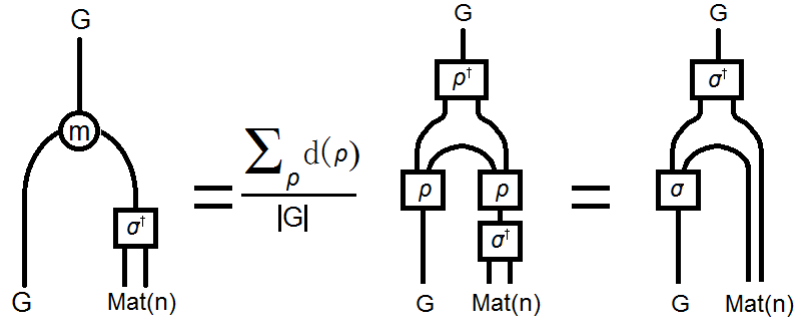
Let G be a group. Linearizing the multiplication function $m : G \times G \rightarrow G$ and unit element $e \in G$, we obtain the following diagrams



For finite group G , the representations are defined by the maps $\rho : G \rightarrow \text{Mat}(n)$ where $\text{Mat}(n)$ is the algebra of $n \times n$ matrices. The representations have the following properties:



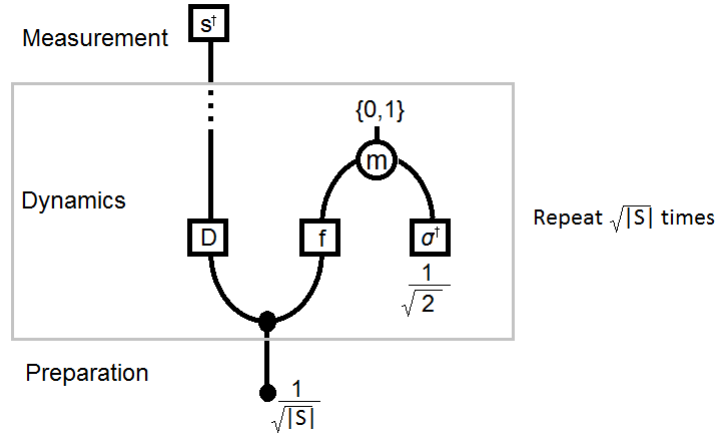
We finalize this section with the following equation which is the result of basic theorems in representation theory (the reader can refer to [7] for detailed explanation):



Here the sum is over equivalence classes of irreducible representations of G and σ^\dagger is adjoint of an irreducible representation.

4. TOPOLOGY OF GROVER ALGORITHM

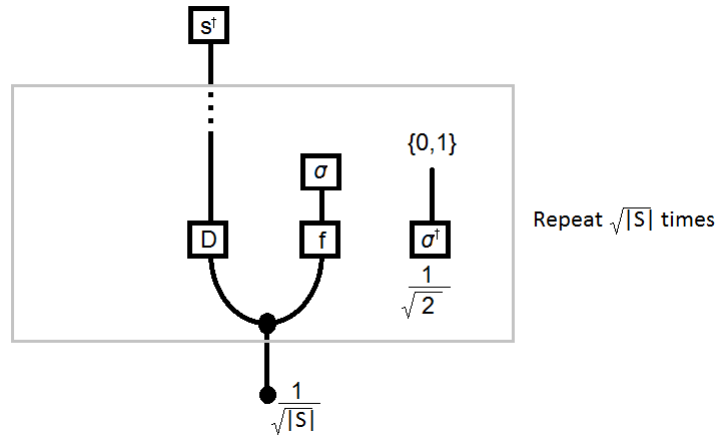
The topological structure of the (multi-step) Grover algorithm as follows:



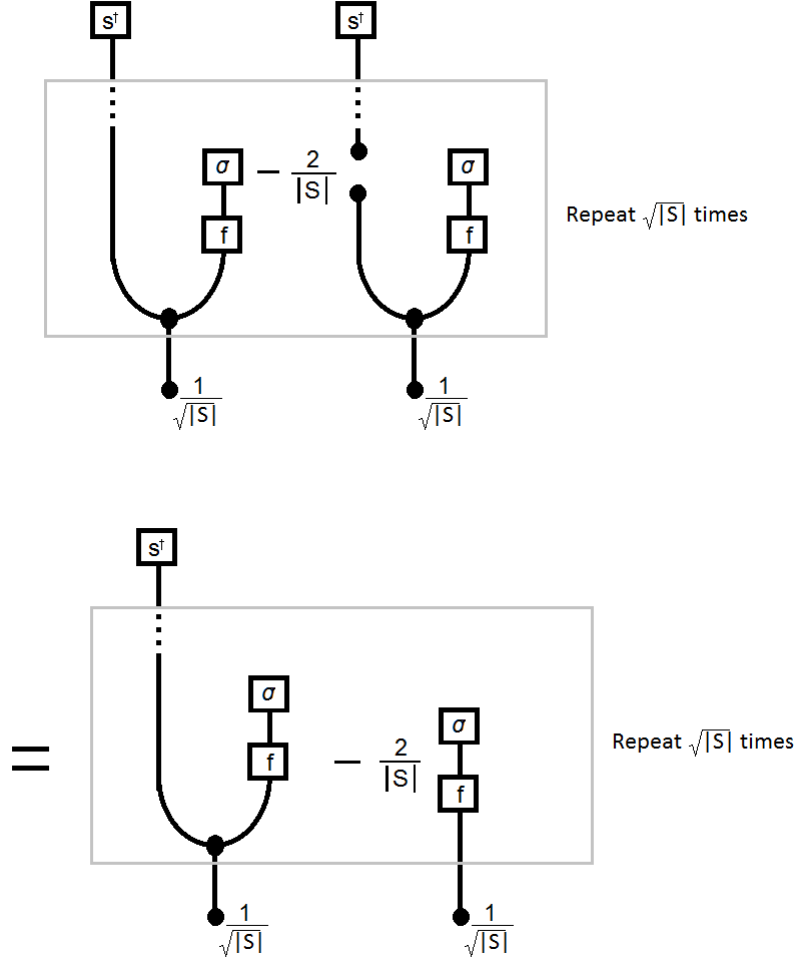
The projective measurement is performed in the base system $|s\rangle$. D corresponding the inversion about the mean (i.e. $-I + 2A$) can be decomposed:

$$\begin{array}{c} S \\ | \\ \boxed{D} \\ | \\ S \end{array} = \begin{array}{c} S \\ | \\ | \\ | \\ S \end{array} - \frac{2}{|S|} \begin{array}{c} S \\ | \\ \bullet \\ | \\ \bullet \\ | \\ S \end{array}$$

Next we use the last identity of the section 3 to convert the algorithm to the following form:

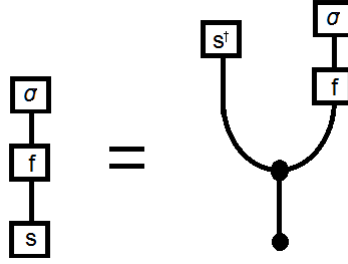


We now neglect second part of this system as it is a product state. Using the decomposition of D we rewrite the system:



The last equality is result of the identities stated in the last section.

It is clear that for the representation σ we have $\sum_{i \in S} \sigma = (|S| - 1) + (-1) = |S| - 2$ as a factor in our final measurement. For an unmarked element s , we obtain the factor $+1$ in the measurement as a result of the following topological identity:



Hence for such an unmarked element we will get the following result:

$$A = \left(\frac{1}{|S|}\right)^{\sqrt{|S|}} \left[\left(1 - \frac{2}{|S|}\right)^{\sqrt{|S|-1}} (|S| - 2)^{\sqrt{|S|-1}} - \frac{2}{|S|} \left(1 - \frac{2}{|S|}\right)^{\sqrt{|S|-1}} (|S| - 2)^{\sqrt{|S|}} \right]$$

Here the first summand in the bracket is the result of the figures which have one s^\dagger box while the second summand is from the figures without any s^\dagger boxes. This result can be simplified to the following expression:

$$A = \left(\frac{1}{|S|}\right)^{\sqrt{|S|}} \left(1 - \frac{2}{|S|}\right)^{\sqrt{|S|-1}} (|S| - 2)^{\sqrt{|S|-1}} \left(-1 + \frac{4}{|S|}\right).$$

Hence A^2 is the probability of measuring an unmarked element. We note that A^2 is less than $1/2$ and approaches to zero as n gets larger. To find the probability for the marked element we now calculate the total probability for unmarked elements. Since there are $2^n - 1$ unmarked elements, we consider the value $(2^n - 1)A^2$. It is straightforward to check this value is less than $1/2$ and actually goes to zero as n gets larger. This implies that the probability of measuring the marked element will be at least $1/2$ after $\sqrt{|S|}$ iterations. This proves the correctness of the algorithm. One can also see the reason why the algorithm is repeated $\sqrt{|S|}$ times by examining the expression A where the power of the terms are the result of the number of the iteration.

5. CONCLUSION

In this paper, we present multi-shot Grover search algorithm using a topological semantics originated from categorical quantum mechanics program. This new method provides a new and simple proof of the Grover algorithm and opens the ways to new generalizations.

REFERENCES

- [1] S. Abramsky and B. Coecke, *A categorical semantics of quantum protocols*, Proceedings of the 19th Annual IEEE Symposium on Logic in Computer Science, pages 415-425, 2004. IEEE Computer Science Press.
- [2] B. Coecke, *The logic of entanglement: An invitation*, Technical Report, University of Oxford, 2003. Computing Laboratory Research Report PRG-RR-03-12.
- [3] B. Coecke and R. Duncan, *Interacting quantum observables: Categorical Algebra and diagrammatics*, New Journal of Physics. **13**(2011).
- [4] L. Grover, *Quantum mechanics helps in searching for a needle in a haystack*, Physical Review Letters, **79**(1997), no. 2, 325-328,
- [5] G. M. Kelly and M. L. Laplaza, *Coherence for compact closed categories*, Journal of Pure and Applied Algebra, **19**(1980), 193-213.
- [6] P. Selinger, *New Structures for Physics, chapter A Survey of Graphical Languages for Monoidal Categories*, 289-355, Number 813 in Lecture Notes in Physics. Springer, 2011.
- [7] J. Vicary, *The Topology of Quantum Algorithms*, Proceedings-Symposium on Logic and Computer Science, art. no. 6571540, pp. 93-102.

DEPARTMENT OF MATHEMATICS, COLLEGE OF SCIENCE, UNIVERSITY OF BAHRAIN, BAHRAIN

E-mail address: `aduman@uob.edu.bh`